Zeitschrift für Datenrecht und Informationssicherheit

digma

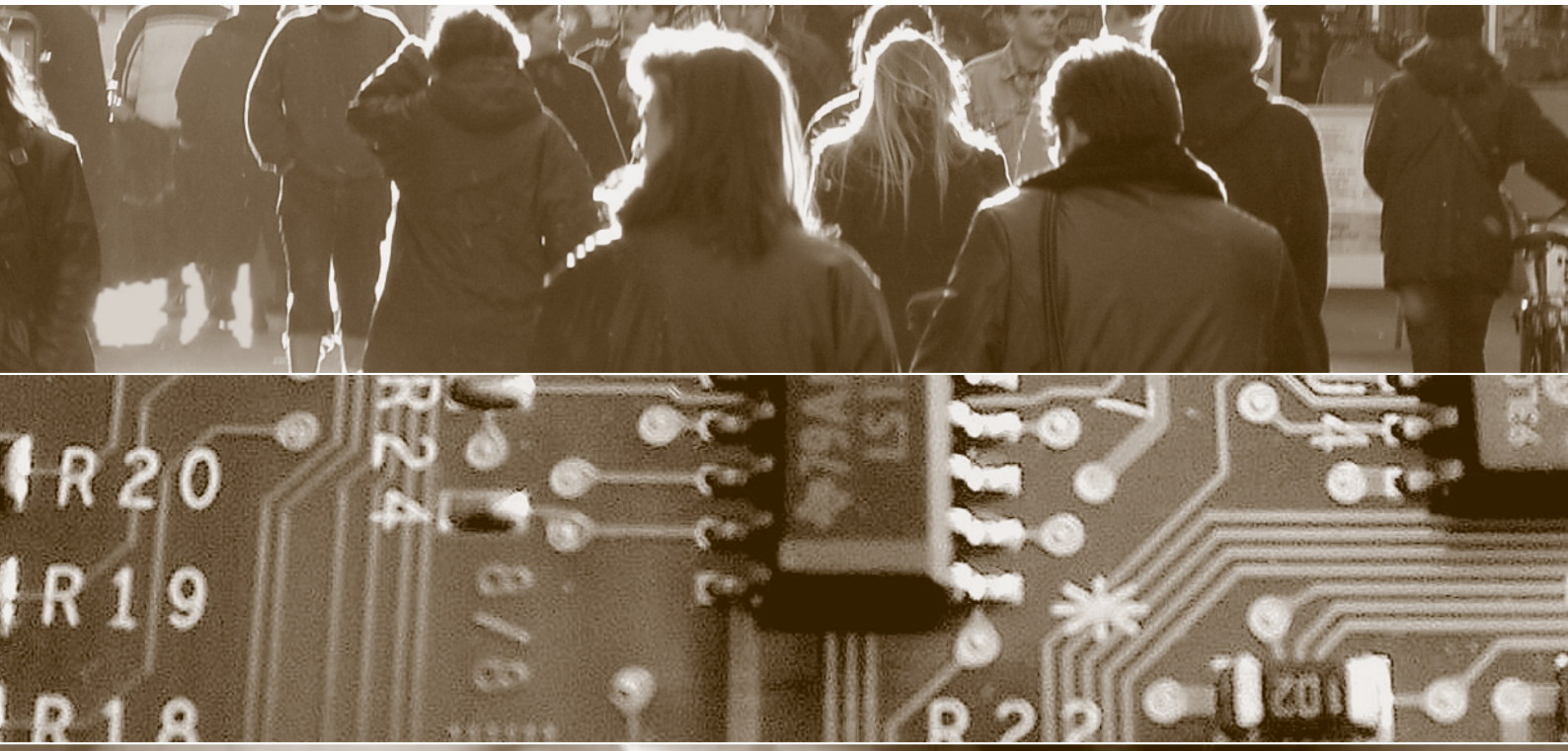
www.digma.info

20. Jahrgang, Heft 4, Dezember 2020

Schwerpunkt:

20 Jahre digma – Lessons learned

fokus: Daten nutzen oder Daten schützen?
fokus: Contact Tracing und Privacy by Design
fokus: Digitalisierung im Gesundheitswesen



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
20 Jahre digma – Lessons learned

Ein Jubiläumsjahr geht zu Ende

Was sagt der Verlagsleiter, der digma 2001 an Bord geholt hat, zur letzten Nummer in der gewohnten Form?

Daten nutzen oder Daten schützen?

Mit der DSG-Revision sollte ursprünglich der Datenschutz gestärkt werden. Ist das gelungen? Sollen, wie etwa verlangt wird, Unternehmen über Personendaten autonom entscheiden dürfen, solange sie keine Person diskriminieren?

Verpasste Chance und Handlungsbedarf

Erkenntnisse aus dem zweiten digma-Jahrzehnt: Bei der DSG-Revision ist die Chance verpasst worden, mit der Entflechtung der Regeln für Private und öffentliche Organe den komplett verschiedenen Rechtfertigungskonzepten Rechnung zu tragen. Und die Datenschutzbehörden sind in vielen Fällen immer noch eher ein Feigenblatt als eine wirksame Aufsicht.

Contact Tracing und Privacy by design

Was vermochte «Privacy by design» beim Contact Tracing zu leisten? Welches sind die Anforderungen an eine datenschutzfreundliche Contact-Tracing-App?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, lic. iur. Ines Weihrauch

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: 4-mal jährlich (März, Juni, September, Dezember)

Bezugsbedingungen: Jahresabonnement: CHF 178.00 (für Studierende: CHF 98.00), Einzelheft: CHF 48.00, zzgl. Versandkosten. Alle Abo-Preise inkl. 2,5% MWST, zzgl. Versandkosten von CHF 6.00 innerhalb der Schweiz (Versandkosten für Lieferung ins Ausland: CHF 31.00). Studentenpreis gegen Vorlage eines gültigen Nachweises. Abonnementkündigungen sind mit einer Frist von 8 Wochen zum Ende des berechneten Bezugsjahres möglich.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa, Tel. +41 (0)44 928 56 17, marc.schaettin@fachmedien.ch

Verlag und Kundenservice: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

report

Pseudonymisierung von Bankkundendaten

Pseudonymisierte Bankkundendaten sind nach jüngster Rechtsprechung aus Sicht des Empfängers weder vom DSG noch vom Bankgeheimnis geschützt, sofern die Re-Identifikation der Kunden wirksam verhindert ist. Welche Vorsichtsmassnahmen sind zu empfehlen, bevor pseudonymisierte Bankkundendaten weitergegeben werden?

forum

Quo vadis KI? Neues Weissbuch der EU

Wie sind gesetzliche Regelungen zur künstlichen Intelligenz (KI) auszugestalten, damit sich das Potenzial wie auch die Gefahren von KI zielführend kanalisieren lassen? Die EU hat dazu ein Weissbuch veröffentlicht. Was plant die Schweiz?

Daten-Schutz-gebiet

Ein neues Datenschutzgesetz sollte den Datenschutz stärken. Fühlen Sie sich im Daten-Schutzgebiet jetzt sicher vor Datenhaien, Datenkraken usw.?

In eigener Sache

Diese vierte Nummer im 20. Jahrgang ist die letzte digma-Nummer in dieser Form. Herausgeber, Redaktion und Verlag danken Ihnen für zwanzig Jahre der Treue, des Interesses und der Unterstützung – und den unzähligen Autorinnen und Autoren für ihre wertvollen Beiträge! Wie es weitergeht, erfahren Sie demnächst unter <https://www.digma.info>.

Aus der Praxis

Pseudonymisierung von Bankkundendaten

Emilie Jacot-Guillarmod, MBA (INSEAD), Rechtsanwältin, Lenz & Staehelin, Redakteurin bei LawInside.ch, Genf*
emilie.jacot-guillarmod@lenzstaehelin.com

Célian Hirsch, Rechtsanwalt, Doktorand am Institut für Bank- und Finanzmarktrecht der Universität Genf, Mitbegründer von LawInside.ch, Genf*
celian.hirsch@lawinside.ch

Die Diskussion rund um die Pseudonymisierung und Anonymisierung von Bankkundendaten[1] ist nicht neu, gelangte jedoch kürzlich mit der Veröffentlichung des Cloud-Leitfadens der Schweizerischen Bankiervereinigung (SBVg) vom März 2019 vermehrt in den Fokus[2]. Gemäss der SBVg gewährleisten Anonymisierung, Pseudonymisierung und Verschlüsselung, dass das Bankgeheimnis und die Datenschutzbestimmungen im Falle einer Speicherung von *«Client Identification Data»* (CID) auf einem Cloud-Server im Ausland eingehalten werden. In der Praxis greifen Banken häufig zu den Mitteln der Anonymisierung oder Pseudonymisierung, um die mit der Auslagerung der Verarbeitung von Kundendaten verbundenen Risiken zu mindern.

Dennoch sind die rechtlichen Folgen von Pseudonymisierung und Anonymisierung weitgehend unklar.

In diesem Beitrag analysieren wir die Entwicklung der Rechtsprechung bezüglich pseudonymisierter Bankkundendaten. Zunächst führen wir aus der Perspektive des Datenschutzes und des Bankgeheimnisses in das Thema ein. Danach untersuchen wir die einschlägige Rechtsprechung. Abschliessend ziehen wir einige Schlussfolgerungen für die Praxis.

Fragestellung

Bezüglich Datenschutz

Sind pseudonymisierte Bankkundendaten Personendaten? Gemäss Art. 3 Bst. a des Datenschutzgesetzes (DSG) sind Personendaten im Sinne des DSG «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen». Ausschlaggebend für die sachliche Geltung des DSG ist somit namentlich die Möglichkeit, die betroffene Person zu identifizieren: Fehlt diese, findet das DSG keine Anwendung.

Bestimmtheit im Sinne von Art. 3 Bst. a DSG bedeutet, dass die Identität der betroffenen Person[3] direkt aus den relevanten Daten ersichtlich ist[4]. Bestimmbarkeit liegt vor, wenn die Daten die Wiedererkennung indirekt (durch Korrelation von Informationen oder aufgrund des Kontextes) ermöglichen[5]. Eine rein theoretische Möglichkeit der Identifizierung reicht nicht aus[6]. Ist der mit der Identifizierung verbundene Aufwand unverhältnismässig gross, so dass ihn eine interessierte Person nach der allgemeinen Lebenserfahrung nicht auf sich nehmen würde, ist die betroffene Person im Sinne des Datenschutzgesetzes nicht bestimmbar[7]. In diesem Zusammenhang werden insbesondere das Interesse an der Identifizierung[8] sowie die zur Verfügung stehenden technischen Mittel (wie z.B. Suchmaschinen)[9] berücksichtigt.

Technische Verfahren[10] können die Wiedererkennung der betroffenen Person verhindern. Der Begriff «Pseudonymisierung» bezieht sich auf Verfahren, bei denen Identifikationsmerkmale durch neutrale Identifikatoren ersetzt werden[11]. Einige befugte Personen behalten die Möglichkeit, die Daten der betroffenen Person erneut zuzuordnen, indem sie den umgekehrten Vorgang durchführen[12]. Im Gegensatz zur Anonymisierung[13] sind also einige Personen in der Lage, die betroffene Person zu re-identifizieren, während andere dies nicht können[14].

Die rechtliche Qualifikation pseudonymisierter Daten ist in der Lehre umstritten. In diesem Zusammenhang stellt sich die Frage, *aus wessen Sicht* die Möglichkeit einer Wiedererkennung der betroffenen Person beurteilt werden sollte[15]. Laut verschiedenen Autoren reicht es aus, wenn nur eine Partei (z.B. entweder der Absender oder der Empfänger von Daten) die betroffene Person identifizieren kann, damit die Daten *erga omnes* als Per-

sonendaten eingestuft werden (sogenannte *absolute* oder *alternative* Theorie)[16]. Nach diesem Ansatz würden pseudonymisierte Daten in jedem Fall Personendaten darstellen, da bestimmte befugte Personen definitionsgemäss in der Lage sind, die betroffene Person zu re-identifizieren. Andere Autoren sprechen sich dagegen dafür aus, dass die Möglichkeit der Identifizierung der betroffenen Person je nach Standpunkt der verschiedenen Parteien differenziert beurteilt wird (sogenannte *relative Theorie*)[17]. Pseudonymisierte Daten würden somit aus der Sicht des für die Pseudonymisierung Verantwortlichen (und anderer, die den Pseudonymisierungsvorgang rückgängig machen können) als Personendaten und aus der Sicht Dritter (z.B. des Empfängers der pseudonymisierten Daten) als Nicht-Personendaten gelten[18].

In der Bankpraxis wird die Pseudonymisierung insbesondere im Zusammenhang mit der Übermittlung von Kundendaten – vor allem ins Ausland – eingesetzt: Die Bank behält dann die Mittel zur Identifizierung der betroffenen Person, während der Empfänger nur Zugang zu Pseudonymen hat. Je nachdem, wie pseudonymisierte Daten rechtlich eingestuft werden, unterliegen solche Übermittlungen den Anforderungen des DSG oder eben nicht.

Bezüglich Bankgeheimnis

Unterliegen pseudonymisierte Bankkundendaten dem Bankgeheimnis? Bei der Beantwortung dieser Frage sind die Grundlagen des Bankgeheimnisses von Bedeutung. Unter dem Bankgeheimnis versteht man die Verpflichtung einer Bank und ihrer Mitarbeiter, alle Informationen geheim zu halten, die ihnen vom Kunden im Rahmen der Geschäftsbeziehung anvertraut oder ihnen in diesem Zusammenhang zur Kenntnis gebracht werden[19]. Das Bankgeheimnis schützt (i) das Bestehen der vertraglichen Beziehung mit einer Bank; (ii) die Kenntnisse, die sich aus der Geschäftsbeziehung zwischen Bank und Kunden ergeben; sowie (iii) alle Transaktionen und Operationen, die die Bank mit ihren Kunden durchführt, unabhängig davon, ob es sich um Bankgeschäfte oder andere Geschäfte handelt[20].

Das Bankgeheimnis beruht auf zwei unterschiedlichen Rechtsquellen[21]:

- Art. 28 ZGB[22];
- Art. 398 Abs. 2 OR[23] beziehungsweise Art. 2 Abs. 1 ZGB bezüglich Bankverträgen, auf die das Auftragsrecht nicht anwendbar ist[24].

Art. 47 des Bankengesetzes, der gelegentlich auch als Grundlage des Bankgeheimnisses bezeichnet wird[25], stellt lediglich die Verletzung der privatrechtlichen Pflicht zur vertraulichen Behandlung von Kundeninformationen unter Strafe[26].

Wie bereits erwähnt, wird die Identifizierung der betroffenen Person anhand ihrer Daten durch die Pseudonymisierung verhindert oder zumindest wesentlich erschwert. Es ist zu prüfen, ob die Pseudonymisierung von Bankkundendaten gleichzeitig auch dazu führt, dass die betreffenden Daten vom Schutz des Bankgeheimnisses ausgenommen sind. Dies wäre dann der Fall, wenn Informationen nur dann vom Bankgeheimnis erfasst sind, wenn sie einer bestimmten oder bestimmbaren Person zuordenbar sind.

Analyse der einschlägigen Rechtsprechung

Datenschutzrechtliche Entscheide

Im BGE 136 II 508 (sogenanntes «Logistep»-Urteil) hat sich das Bundesgericht über den Begriff «Bestimmbarkeit» zum ersten Mal im Detail geäussert. Es untersuchte den folgenden Sachverhalt: Die Logistep AG zeichnete mittels einer *Ad-hoc-Software* bestimmte Informationen im Zusammenhang mit dem Download urheberrechtlich geschützter Werke aus *Peer-to-Peer*-Netzwerken auf. Darunter befand sich insbesondere die IP-Adresse des für den Download verwendeten Internetanschlusses. Logistep verkaufte diese Informationen an die Urheberrechtsinhaber. Diese reichten gestützt auf die von Logistep zur Verfügung gestellten Daten eine Strafanzeige gegen unbekannt ein. Die Einsicht in die Strafakte ermöglichte es ihnen dann, den Urheberrechtsverletzer zu identifizieren und anschliessend zivilrechtlich gegen ihn vorzugehen.

Kurz & bündig

Die Rechtsnatur pseudonymisierter Bankkundendaten ist lange unklar geblieben. Nach jüngster Rechtsprechung sind solche Daten prinzipiell aus Sicht des Empfängers weder vom DSG noch vom Bankgeheimnis geschützt, sofern die Pseudonymisierung die Wiedererkennung der betroffenen Kunden wirksam verhindert. Angesichts der einschlägigen Rechtsprechung sind jedoch bestimmte Vorsichtsmassnahmen (namentlich eine gründliche Risikobewertung) vor der Weitergabe pseudonymisierter Bankkundendaten empfehlenswert.

In diesem Zusammenhang untersuchte das Bundesgericht die Handlungen von Logistep auf ihre Vereinbarkeit mit dem DSG. In diesem Zusammenhang musste es prüfen, ob Logistep Personendaten im Sinne des DSG bearbeitete. Die Logistep argumentierte hauptsächlich, dass sie selbst nicht in der Lage sei, die betroffenen Personen anhand der gesammelten Daten (insbesondere IP-Adressen) zu identifizieren. Dies sei nur den Urheberrechtsinhabern im Rahmen eines Strafverfahrens möglich[27].

Das Bundesgericht verwarf diese Argumentation von Logistep, wonach sich die Identifizierbarkeit grundsätzlich aus dem besonderen Beurteilungshorizont des Dateninhabers beurteile[28]. Im Zusammenhang mit der Übermittlung von Informationen reicht es gemäss Bundesgericht aus, dass die betroffene Person für den Datenempfänger identifizierbar ist, damit die Daten für *beide an der Übermittlung beteiligten Parteien*[29] Personendaten darstellen. Folglich handelte es sich bei den von Logistep bearbeiteten Daten um Personendaten.

Eine wichtige Weiterentwicklung der Rechtsprechung stellen Entscheide im Rahmen des US-Programms dar, die sich direkt mit Pseudonymisierung befassten. Kürzlich prüften das Zürcher Handelsgericht und (auf Beschwerde hin) das Bundesgericht die Zulässigkeit der Übermittlung pseudonymisierter Daten durch eine Schweizer Bank an das US-Justizministerium («DoJ») im Rahmen des Programms zur Beilegung des Steuerstreits der Schweizer Banken mit den USA («US-Programm»).

In diesem Zusammenhang übermittelte die Bank dem DoJ verschiedene Daten in Bezug auf jeden *closed US-related Account* (d.h. jedes sogenannte Konto mit US-Bezug, das während des vom US-Programm abgedeckten Zeitraums geschlossen wurde), einschliesslich des Namens des zuständigen *Relationship-Managers,* bestimmter Zahlungsverkehrsinformationen und der Art der Beziehung zwischen dem Konto und der US-Person (z.B. Kunde oder wirtschaftlich Berechtigter)[30]. Unter Bezugnahme auf den relevanten Absatz des US-Programms wird diese Information häufig als «II.D.2-Liste» bezeichnet.

Die II.D.2-Listen enthielten keine Informationen, die eine Identifizierung des Kunden direkt ermöglicht hätten. Daten wie der Name des Kunden und die Kontonummer wurden durch Pseudonyme ersetzt[31]. Die Bank war allerdings in der Lage, die Angaben in der II.D.2-Liste anhand einer Korrespondenztabelle den konkreten Kunden zuzuordnen; dies insbesondere im Hinblick auf ein allfälliges späteres Steueramtshilfeersuchen der Vereinigten Staaten. Anlass zu den einschlägigen Entscheiden gab der Antrag des Inhabers und wirtschaftlichen Berechtigten eines geschlossenen US-Kontos, der Bank die Übertragung der Liste II.D.2 zu verbieten.

In seinem Urteil HG150170 vom 30. Mai 2017 entschied das Handelsgericht des Kantons Zürich, dass pseudonymisierte Daten *für eine Person, die keinen Zugang zur Korrespondenztabelle hat*[32], keine Personendaten darstellen, soweit die Pseudonymisierungsmassnahmen die Identifizierung der betroffenen Person wirksam verhindern. Das Bundesgericht stimmte dieser Argumentation zu[33].

Das Handelsgericht analysierte sodann die Re-Identifizierbarkeit des Kunden. Es hielt die von der Bank getroffenen Pseudonymisierungsmassnahmen[34] für unzureichend, um eine Re-Identifizierung im vorliegenden Fall zu verhindern[35]. Diese Massnahmen seien dem DoJ bekannt, einige sogar ausdrücklich im US-Programm vorgesehen[36]. Auch wenn die von der Bank übermittelte II.D.2-Liste keine direkt identifizierenden Informationen (wie z.B. den Namen des Kunden) enthalte, würden bestimmte Daten, insbesondere der Name des für das Konto verantwortlichen *Relationship-Managers,* im Klartext angezeigt. Nach Ansicht des Handelsgerichts schufen diese Informationen zusammen mit den anderen zur Verfügung gestellten Daten einen tauglichen Anknüpfungspunkt zur Identifizierung des Kunden[37].

Das Bundesgericht war diesbezüglich weniger streng[38]. Es stellte fest, dass die durch die Bank vorgenommen Pseudonymisierungsmassnahmen in der Praxis anerkannt sind[39]. Die blosse Tatsache, dass das DoJ davon wusste, schade ihrer Wirksamkeit nicht[40]. Das Bundesgericht war jedoch der Auffassung, dass die Bank ihre Beschwerde gegen das Vorhandensein eines tauglichen Anknüpfungspunkts zur Re-identifizierung (d.h. des unverschlüsselt übermittelten Namens des Kundenbetreuers) nicht hinreichend begründet hatte[41]. Mangels genügender Rüge ging es darauf nicht ein. Deshalb bestätigte das Bundesgericht den handelsgerichtlichen Entscheid, wonach der Kunde und der wirtschaftlich Berechtigte anhand der Angaben in der II.D.2-Liste bestimmbar seien[42].

Unseres Erachtens ist diese theoretische Klarstellung, dass pseudonymisierte Daten *für den Empfänger, der keinen*

Zugriff auf den Korrespondenzschlüssel hat, grundsätzlich keine Personendaten darstellen, zu begrüssen[43]. Die Mehrheit der Lehre hatte zwar die Tragweite des Logistep-Entscheids relativiert[44], jedoch behauptete der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte («Beauftragter»), dass pseudonymisierte Daten gestützt auf den Logistep-Entscheid stets als Personendaten einzustufen seien[45]. Diese Stellungnahme des Beauftragten war unserer Meinung nach im Hinblick auf die *ratio legis* des Datenschutzgesetzes unangemessen streng: Die Übermittlung von Daten, die keine Identifizierung durch den Empfänger ermöglichen, verletzt die Persönlichkeitsrechte der betroffenen Person nicht. Die oben erwähnte Rechtsprechung bezüglich des US-Programms stellt somit eine begrüssenswerte Entwicklung dar, indem sie klarstellt, dass (wirksam) pseudonymisierte Daten für den Empfänger prinzipiell keine Personendaten darstellen.

Dennoch vermag diese Rechtsprechung im Ergebnis nicht zu überzeugen, weil sie darauf abstellt, dass der Kunde allein aufgrund der Übermittlung des Namens des *Relationship-Managers* im Klartext durch das DoJ identifizierbar sei, obwohl die anderen Daten ausreichend pseudonymisiert sind. Wir möchten an dieser Stelle betonen, dass das Bundesgericht die diesbezügliche Analyse des Handelsgerichts aus einem prozessualen Grund bestätigt hat, nämlich mangels hinreichend begründeter Rüge. Unseres Erachtens können daher keine allgemeinen Schlussfolgerungen daraus gezogen werden, ausser dass bei der Übermittlung bestimmter Daten im Klartext besondere Vorsicht geboten ist.

Entscheide hinsichtlich des Bankgeheimnisses

Soweit ersichtlich, hat die Rechtsprechung bisher nie ausdrücklich entschieden, inwieweit sich das Bankgeheimnis auch auf Bankkundendaten bezieht, die keiner bestimmten oder bestimmbaren Person zugeordnet werden können. In BGE 141 III 119 äusserte sich das Bundesgericht in wenigen Worten zur Identifizierbarkeit des Kunden als Kriterium zur Anwendung des Bankgeheimnisses[46]. Gemäss Bundesstrafgericht sind Informationen, die die Identifizierung von Kunden von Schweizer Banken ermöglichen – unabhängig davon, ob sie sich im Besitz der Bank, eines Anwalts oder eines Bevollmächtigten befinden – durch die schweizerische öffentliche Ordnung geschützt[47]. *E contrario* würde dies heissen, dass Daten, die keine Wiedererkennung des Kunden erlauben, durch das Bankgeheimnis nicht geschützt sind.

In dem bereits erwähnten Urteil HG150170 vom 30. Mai 2017 stellte das Handelsgericht fest, dass die strittigen Daten ursprünglich (d.h. vor ihrer Pseudonymisierung) durch das Bankgeheimnis geschützt waren[48]. Dann prüfte es, ob die Bank die Daten anonymisiert oder pseudonymisiert hatte[49]. Die Übermittlung von wirksam anonymisierten oder pseudonymisierten Daten würde nach Ansicht des Handelsgerichts nämlich keine Offenbarung des (Bank-)Geheimnisses darstellen[50]. Es sei an dieser Stelle darauf hingewiesen, dass sich das Bundesgericht in seinem Urteil zu dieser Frage nicht geäussert hat.

In dieser Hinsicht überzeugt der handelsgerichtliche Entscheid[51]. In der Tat beruhen das Bankgeheimnis und das Datenschutzgesetz auf derselben Grundlage: dem Persönlichkeitsschutz. Soweit pseudonymisierte Bankkundendaten keine Identifizierung ermöglichen, stellt die Einschränkung der Übermittlung oder Offenlegung solcher Daten somit keinen zusätzlichen Schutz der Persönlichkeit der betroffenen Person dar. Dies gilt sowohl im Rahmen des Datenschutzgesetzes als auch des Bankgeheimnisses. Demzufolge sind Bankkundendaten, die wirksam (d.h. in einer Weise, die es einem Dritten[52] verunmöglicht, die betroffene Person ohne unverhältnismässigen Aufwand zu re-identifizieren) pseudonymisiert oder anonymisiert sind, nicht durch das Bankgeheimnis geschützt.

Diese Schlussfolgerung entspricht auch Rundschreiben[53] und Entscheiden der FINMA[54] sowie der Lehre zum Berufsgeheimnis (Art. 321 StGB)[55].

Praktische Bedeutung

Die oben dargelegten Klarstellungen der Rechtsprechung bezüglich der Rechtsnatur von pseudonymisierten Bankkundendaten sind zu begrüssen. Wie vorstehend erwähnt, erscheint uns die Schlussfolgerung, wonach solche Daten weder dem Datenschutz noch dem Bankgeheimnis unterstehen, begründet, da der Persönlichkeitsschutz die gemeinsame Grundlage dieser beiden Rechtsgebiete bildet.

Wichtig für die Praxis ist die Aufteilung der Beweislast. Es ist an dieser Stelle darauf hinzuweisen, dass es gemäss den oben genannten Entscheiden der Bank obliegt, nachzuweisen, dass die Pseudonymisierung die erneute Identifizierung der betroffenen Person tatsächlich verhindert[56]. Nach dem heutigen Stand der Rechtsprechung müssen Banken, die anonymisierte oder pseudonymisierte Bankkun-

dendaten ins Ausland übermitteln wollen, daher das Risiko einer Re-Identifikation im Detail analysieren, dieses Risiko in geeigneter Weise mindern und diesen Prozess ausreichend dokumentieren, damit sie in einem allfälligen Rechtsstreit den erforderlichen Beweis erbringen können. Insbesondere erachten wir die folgenden Mindestvorkehrungen als empfehlenswert:

- die Bank sollte den Zugriff auf den Identifikationsschlüssel auf diejenigen Personen beschränken, die ihn benötigen *(Need-to-know-Prinzip).* Der Schlüssel sollte vor unberechtigtem Zugriff geschützt werden. Diese Massnahmen sind zu dokumentieren;
- die Bank sollte durch technische Tests bestätigen, dass die Identität des Kunden nicht aus den übermittelten Daten abgeleitet werden kann (etwa durch eine Verknüpfung der übermittelten Daten miteinander). Die angewandte Methode und die Testergebnisse sind zu dokumentieren;
- die Bank sollte die Datenzugriffsrechte von Dritten (insbesondere lokalen Behörden) im Zielland berücksichtigen;
- die Bank sollte das Risiko analysieren, dass der Empfänger und/oder ein berechtigter Dritter den Kunden durch Verknüpfung der übermittelten Daten mit anderen ihnen zur Verfügung stehenden Daten re-identifizieren können (Verknüpfung mit anderen Datenbanken). In diesem Zusammenhang erachten wir es als notwendig, insbesondere die Art und den Umfang anderer Informationen, die dem Datenempfänger und/oder dem betreffenden Dritten wahrscheinlich zur Verfügung stehen, sowie die Relevanz der Re-Identifikation für diese Interessenten zu berücksichtigen;
- je nach Risiko einer Re-Identifizierung sollte die vorherige Zustimmung des Kunden zur betreffenden Datenübermittlung sowie zur Aufhebung des Bankgeheimnisses eingeholt werden – etwa durch die Überarbeitung der allgemeinen Geschäftsbedingungen der Bank.

Schlusswort

Nach neuerer Rechtsprechung stellen pseudonymisierte Bankkundendaten für Personen, die keinen Zugang zum Korrespondenzschlüssel haben, keine Personendaten oder keine bankgeheimnisgeschützten Informationen dar. Dies ist eine wichtige Entwicklung in der Rechtsprechung, da diese Fragen bisher wenig thematisiert wurden und das Bundesgericht in seinen seltenen früheren Entscheiden zu diesem Thema einen konservativeren Ansatz verfolgte.

Dennoch birgt die Offenlegung von pseudonymisierten Bankkundendaten Risiken für die Bank. Es liegt in der Verantwortung der Bank, sicherzustellen – und im Streitfall zu beweisen –, dass die Pseudonymisierungsmassnahmen ausreichend sind. Wir hoffen, dass künftige Gerichtsurteile den Umfang der von der Bank zu liefernden Beweise angemessen beschränken werden, insbesondere im Hinblick auf negative Tatsachen. Nach heutigem Stand der Rechtsprechung trägt indessen die Bank weitgehend allein die diesbezügliche Beweislast[57].

Unter diesen Umständen sind wir der Meinung, dass es aus Gründen der Vorsicht geboten ist, vor der Datenübermittlung eine Analyse der mit der Verarbeitung verbundenen Risiken durchzuführen und verschiedene Vorsichtsmassnahmen zu treffen. In den vorangegangenen Absätzen geben wir einige entsprechende Empfehlungen für die Praxis. ■

Fussnoten

* Die Autoren danken Martina Reber (Rechtsanwältin, Doktorandin) und Nino Sievi (Dr. iur, Rechtsanwalt) sehr herzlich für ihre sorgfältige Überprüfung und ihre wertvollen Kommentare.

1 Eine detailliertere, auf Französisch verfasste Version dieses Aufsatzes ist in der SZW 2020 erschienen: Hirsch Célian/Jacot-Guillarmod Emilie, *Les données bancaires pseudonymisées – Du secret bancaire à la protection des données,* in: SZW 2020, 151 ff.

2 Die Schweizerische Bankiervereinigung (SBVg) hat im Juni 2020 eine 2. Auflage des Cloud-Leitfadens herausgegeben (SBVg, *Cloud-Leitfaden – Wegweiser für sicheres Cloud Banking,* 2. Aufl., Juni 2020) vgl. auch die von der SBVg in Auftrag gegebenen und im Jusletter vom 27. Mai 2019 veröffentlichten Rechtsgutachten (Laux Christian/Hofmann Alexander/Schieweck Mark/Hess Jürg, Nutzung von Cloud-Angeboten durch Banken, in: Jusletter 27. Mai 2019; Isler Michael/Kunz Oliver M./Müller Thomas/Schneider Jürg/Vasella David, Bekanntgabe von Bankkundendaten an Beauftragte im In- und im Ausland, in: Jusletter 27. Mai 2019).

3 De lege lata stellen sowohl Daten, die natürliche Personen betreffen, als auch Daten, die sich auf juristische Personen beziehen, Personendaten dar (Art. 3 Bst. b DSG). Der Entwurf zur Totalrevision des DSG (nachfolgend «E-DSG») schlägt vor, auf den Schutz von Daten juristischer Personen zu verzichten, was einer schweizerischen Besonderheit ein Ende setzen würde (Art. 4 Bst. a E-DSG). Siehe auch die Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7011.

4 Botschaft des Bundesrates zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 413, 444 (nachfolgend «Botschaft DSG»); BGE 138 II 346 E. 6.1; BGE 136 II

Fussnoten (Fortsetzung)

508 E. 3.2; Bundesverwaltungsgericht, A-7183/2008 vom 7. Mai 2009, E. 5.2.2; Blechta, in: Maurer-Lambrou/Blechta (Hrsg.), BSK-DSG/BGÖ – Basler Kommentar Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl. (nachfolgend BSK-DSG/BGÖ-Autor[-in]), Art. 3 DSG N 8 ff.; Meier Philipp, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, N 431 ff.; Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, 2008, Art. 3 DSG N 20. Beispielsweise ermöglicht ein Personalausweis die direkte Identifizierung der betroffenen Person (BGE 138 II 346 E. 6.1). Dasselbe gilt nach Probst für eine Visitenkarte (Probst Thomas, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Personen im Datenschutzrecht, in: AJP 2013 1423 ff. (nachfolgend Probst Thomas, Bestimmbarkeit, 1429 ff.).

5 Ebd. So kann es beispielsweise möglich sein, die auf einem Foto erscheinende Person trotz Verwischung ihres Gesichts angesichts des Ortes und/oder Kontextes zu identifizieren (BGE 138 II 346 E. 6.2 ff.). Eine IP-Adresse ermöglicht es unter bestimmten Umständen, die betroffene Person zu identifizieren (BGE 136 II 508 E. 3.5), siehe auch infra Abschnitt 3.a.i. Aus der Sicht des Europarechts siehe EuGH, Urteil vom 19. Oktober 2016, C-582/2014, Patrick Breyer gegen Deutschland.

6 Ebd.

7 Botschaft DSG (Fn. 4), 452; BGE 138 II 346 E. 6.1; BGE 136 II 508 E. 3.2; Bundesverwaltungsgericht, A-7183/2008 vom 7. Mai 2009, E. 5.2.2; BSK-DSG/BGÖ-Blechta (Fn. 4), Art. 3 DSG N 11; Rosenthal/Jöhri (Fn. 4), Art. 3 DSG N 24 ff.; Rosenthal David, Personendaten ohne Identifizierbarkeit? in: digma 2017, 198 ff., 199 ff.; Meier (Fn. 4), N 433. Beispielsweise ist die betroffene Person in der Regel nicht bestimmbar, wenn ihre Identifizierung die komplizierte Analyse einer Statistik erfordern würde (Botschaft DSG [Fn. 4], 445).

8 Ebd. So ist der erfolglose Kandidat für die diplomatische Prüfung aufgrund der offiziellen Korrespondenz, die sich allgemein auf das Auswahlverfahren für Diplomaten bezieht, nicht bestimmbar, wenn die Identifizierung eine Gegenprüfung der in dieser Korrespondenz enthaltenen Informationen mit einer vertraulichen Kandidatenliste voraussetzen würde. Tatsächlich scheint im Hinblick auf das Interesse an der Identifizierung für einen Dritten ein solcher Aufwand unzumutbar (Bundesverwaltungsgericht, A-7183/2008 vom 7. Mai 2009). Im Gegensatz dazu stellt die Einleitung eines Strafverfahrens gegen eine unbekannte Person zur Identifizierung eines Urheberrechtsverletzers einen Aufwand dar, der nach allgemeiner Lebenserfahrung von einem Urheberrechtsinhaber unter Umständnen umgesetzt werden wird (BGE 137 II 508 E. 3.5). Es ist darauf hinzuweisen, dass nicht immer klar ist, von welchem Standpunkt aus die Identifizierungsmöglichkeit analysiert wird (für eine Zusammenfassung der Probleme und Standpunkte, die in Lehre und Rechtsprechung vertreten werden, vgl. Probst [Fn. 4], Bestimmbarkeit, 1431 ff.). Als Beispiel erwähnt Probst die Versicherungsnummer (in der Alltagssprache oft als «AHV-Nummer» bezeichnet): Die Versicherungsnummer ist heute eine Folge von Zufallszahlen. Die Möglichkeit, die betroffene Person zu identifizieren, hängt somit von den übrigen verfügbaren Informationen ab. Deshalb fällt die Analyse unterschiedlich aus, je nachdem, ob man den Standpunkt des Arbeitgebers der betroffenen Person oder den eines Dritten einnimmt (Probst, Bestimmbarkeit [Fn. 4], 1426).

9 Ebd. Die erste Überlegung ist die Möglichkeit eines Abgleichs mit anderen Informationsquellen; vgl. Probst Thomas, Die Verknüpfung von Personendaten und deren Tragweite, in: Datenverknüpfung, Problematik und rechtlicher Rahmen, Epiney/Probst/Gammenthaler (Hrsg.), Zürich/Basel/Genf 2011 (nachstehend: Probst, Verknüpfung), 19; sowie Probst, Bestimmbarkeit (Fn. 4), 1425. Die entsprechenden Mittel können jedoch auch den Rückgriff auf eine dritte Partei, einschliesslich einer Behörde, umfassen (BGE 136 II 508 E. 3.5 und darin angeführte Quellen). So ist die Einleitung eines Strafverfahrens gegen eine unbekannte Person unter bestimmten Umständen ein zumutbares Mittel zur Identifizierung des Inhabers einer IP-Adresse (BGE 136 II 508 E. 3.5).

10 Z.B.Verschlüsselung.

11 Z.B. das Ersetzen eines Namens durch einen Alias oder durch eine Nummer. Meier (Fn. 4), N 446; Probst, Verknüpfung (Fn. 9), 17; Rosenthal/Jöhri (Fn. 4), Art. 3 DSG N 36 f.; Schweizer Rainer J./Bischof Severin, Der Begriff der Personendaten, in: digma 2011, 152 ff., 156.

12 Z.B. durch Bezugnahme auf eine Konkordanztabelle zwischen Pseudonym und Identifikationsmerkmale oder mittels eines Zweiwege-Verschlüsselungsalgorithmus, siehe Meier (Fn. 4), N 446.

13 Anonymisierung bezweckt, die Wiedererkennung der betroffenen Person zu verhindern, und zwar auch durch den für die Datenverarbeitung Verantwortlichen. Soweit die Anonymisierung per definitionem die Re-Identifikation der betroffenen Person unmöglich macht, stellen anonymisierte Daten keine Personendaten dar und fallen nicht in den Geltungsbereich des DSG (Baeriswyl, Big Data zwischen Anonymisierung und Re-Individualisierung, ZIK 59/2014, 50 ff.; Probst, Verknüpfung (Fn. 9), 13 ff.; Rosenthal/Jöhri (Fn. 4), Art. 3 DSG N 35; Rudin, in: Baeriswyl/Pärli (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz (DSG), Bern 2015 (fortan: SHK-DSG-Autor[-in]), Art. 3 N 13; Schweizer/Bischof [Fn. 11], 155). Probst stellt fest, dass, obwohl Anonymisierung nicht gesetzlich definiert ist, manche gesetzlichen Bestimmungen die Anonymisierung von Daten verlangen, z.B. Art. 9 BGÖ, Art. 14a BStatG und Art. 12 Volkszählungsgesetz.

14 Probst, Verknüpfung (Fn. 9), 17; SHK-DSG-Rudin (Fn. 13), Art. 3 N 14.

15 Probst, Bestimmbarkeit (Fn. 4), 1426.

16 Die europäischen Datenschutzbehörden sprechen sich für die absolute Theorie aus, vgl. Stellungnahme 05/2014 der Artikel 29 Datenschutzgruppe, 10 und 16 ff. Uns sind keine Schweizer Autoren bekannt, die sich ausdrücklich für die alternative Betrachtungsweise aussprechen. Der Beauftragte hat sich jedoch für die Anwendung der alternativen Betrachtungsweise in Bezug auf pseudonymisierte Daten ausgesprochen, vgl. 22. Tätigkeitsbericht des Beauftragten (2014/2015) – Auslagerung von pseudonymisierten Bankkundendaten ins Ausland (<https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activities/formreports/22e-rapport-d-activities-2014-2015/externalisation-a-letranger-de-donnees-bancaires-pseudonymisees.html>).

17 In diesem Sinne z.B. Probst, Bestimmbarkeit (Fn. 4), 1429 ff.; SHK-DSG-Rudin (Fn. 13), Art. 3 DSG N 12.

18 Ebd.

19 BGE 145 IV 114 E. 3.3.2; vgl. auch BGE 137 II 431 E. 2.1; Aubert Maurice et al., Le secret bancaire suisse, Bern 1995, 43.

20 HG150170, E. 5.3.4.2; FINMA-Bulletin 4/2013, 73 ff.; Lombardini Carlo, Droit bancaire suisse, 2. Aufl., Zürich/Basel/Genf 2008, 967 ff.

21 BGE 145 IV 114 E. 3.3.2; Aubert et al. (Fn. 19), 52 ff.; BSK BankG, Stratenwerth Günter, Art. 47 BankG N 1; Lombardini (Fn. 20), 965 ff. Das Bankgeheimnis ist ebenfalls durch die Verfassung geschützt (Art. 13 BV), obwohl es nicht den Status eines Grundrechts hat (Biaggini Giovanni, in: BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2 Aufl., Zürich 2017, Art. 13 BV N 1a).

Fussnoten (Fortsetzung)

22 Art. 28 ZGB sieht vor, dass eine Person, die in ihrer Persönlichkeit widerrechtlich verletzt wird, zu ihrem Schutz das Gericht anrufen kann. Wie der Datenschutz beruht somit auch das Bankgeheimnis auf dem Schutz der Privatsphäre.

23 Gemäss Art. 398 Abs. 2 OR haftet der Beauftragte gegenüber dem Auftraggeber für die ordnungsgemässe und getreue Ausführung des Auftrags.

24 Art. 2 Abs. 1 ZGB sieht vor, dass jedermann in der Ausübung seiner Rechte und in der Erfüllung seiner Pflichten nach Treu und Glauben zu handeln hat.

25 Lombardini (Fn. 20), 965 ff.

26 BGE 145 IV 114 E. 3.3.2.

27 BGE 136 II 508 E. 2.2. Die an der Übermittlung beteiligten Parteien hatten somit unterschiedliche Mittel zur Identifizierung. In diesem Sinne weist die faktische Situation, die zum Logistep-Urteil führte, Ähnlichkeiten mit der Übermittlung pseudonymisierter Daten auf.

28 BGE 136 II 508 E. 3.4 und darin angeführte Referenzen.

29 Ebd. Das Bundesgericht hat die Möglichkeit der Identifizierung im Einzelfall bestätigt, da die erforderlichen Schritte in keinem Missverhältnis zu den auf dem Spiel stehenden Interessen standen (BGE 136 II 508 E. 3.5). Es betont auch, dass das Geschäftsmodell von Logistep gerade auf der Möglichkeit der Identifizierung beruhte (ebd.). Vgl. in diesem Zusammenhang auch oben Fn. 8. Für eine Diskussion anderer im Logistep-Urteil angesprochener Datenschutzfragen siehe z.B. Glarner Andreas/Rüfenacht Karin, (Pyrrhus-)Sieg für den Datenschutz, in: Jusletter vom 20. Dezember 2010; und Rosenthal David, Wenn Datenschutz übertrieben wird oder: Hard cases make bad law, in: Jusletter vom 27. September 2010, N 6 ff.; Rosenthal David, Logistep: Offenbar ein Einzelfall, digma 2011 S. 40 ff. Hinsichtlich der Verwendbarkeit von Beweismitteln in Strafverfahren, die durch ähnliche wie die von Logistep angesetzten Methoden gewonnen wurden, siehe Urteil des Berner Obergerichts vom 22. März 2011, BK 11/9, CAN 2012/36 102 ff. Das Obergericht des Kantons Zürich hat die Frage im Urteil vom 3. Februar 2014 (ZR 2014 34 ff.) offengelassen. Zu den Auswirkungen des Logistep-Urteils auf die Haftung von Internetdienstanbietern siehe Francey Julien, La responsabilité délictuelle des fournisseurs d'hébergement et d'accès Internet, N 647 ff.

30 US Programm, Rn. II.D.2.

31 US Programm, Rn. II.D.2; vgl. z.B. die Musterverfügung des Bundesrates vom 3. Juli 2013 und die Erläuterung, wonach die Bewilligung die Übermittlung von Bankkundendaten, verstanden als «persönliche Identifikationsmerkmale des Bankkunden (Name, Adresse, Sozialversicherungsnummer, Kontonummer)» nicht zulässt, abrufbar unter <https://www.newsd.admin.ch/newsd/message/attachments/31820.pdf>.

32 HG150170, E. 5.3.5.2 und 6.

33 BGer 4A_365/2017 vom 26. Februar 2018, E. 5.2.2. Diese Würdigung scheint in der Praxis weitgehend unumstritten. So bestritt der Kläger in einem späteren Rechtsstreit im Rahmen des US-Programmes die Zulässigkeit der Übermittlung pseudonymisierter Daten nicht, sondern nur die Wirksamkeit der von der beklagten Bank getroffenen Pseudonymisierungsmassnahmen (BGer 4A_50/2019 vom 28. Mai 2019, E. 6.5).

34 Nämlich die Ersetzung der Kontonummer durch eine interne Kontrollnummer und die Angabe der gesamten monatlichen Zahlungen, die vom Konto geleistet wurden, in US-Dollar und abgerundet auf die nächsten 10000 USD.

35 HG150170, E. 5.3.5.5.

36 Ebd. Siehe US-Programm, Rn. II.D. 2.

37 Ebd.

38 BGer 4A_365/2017, E. 5.3.1.

39 Ebd.

40 BGer 4A_365/2017, E. 5.3.2.

41 Ebd.

42 Ebd.

43 In dem hier diskutierten Urteil 4A_365/2017 wendete sich das Bundesgericht nicht ausdrücklich von der Logistep-Rechtsprechung ab. Es ist daher nicht auszuschliessen, dass das Bundesgericht unter besonderen Umständen (wie denjenigen, die zum Logistep-Urteil geführt haben) die Möglichkeit einer Re-Identifikation nach der alternativen Betrachtungsweise analysieren könnte.

44 Siehe z.B. Probst, Bestimmbarkeit (Fn. 4), 1429 ff.; Rosenthal David, Logistep: Offenbar ein Einzelfall, digma 2011, 40 ff., 40 f.

45 22. Tätigkeitsbericht von EdöB (2014/2015) (Fn. 16).

46 BGE 141 III 119 E. 5.3; dieser BGE befasst sich mit dem Zugriffsrecht von Bankmitarbeitern auf sie betreffende Daten (d.h. Nicht-Kundendaten), die an die US-Behörden übermittelt wurden. Die Bank begründete ihre Verweigerung des Zugangs zu den angeforderten Dokumenten damit, dass diese die Identifizierung der Kunden ermöglichten und damit Art. 47 BankG verletzt würde (für eine Zusammenfassung von BGE 141 III 119 siehe Schürch Simone, Les données d'employés d'une banque transmises aux autorités américaines, in <http://www.lawinside.ch/14/>).

47 Bundesstrafgericht, SK.2017.64 vom 9. Mai 2018, E. 4.2.7; für eine Diskussion dieses Urteils siehe Villard Katia, Transmission de données clients aux USA: Guilty or not guilty?, veröffentlicht am 5. September 2018 vom Center for Banking and Financial Law, <https://www.cdbf.ch/1022/>; Hirsch Célian, La transmission directe d'informations concernant les clients au Gouvernement américain, in: <http://www.LawInside.ch/646/>.

49 HG150170, E. 5.3.4.6.

49 HG150170, E. 5.3.5.5; zu beachten ist, dass sich das Handelsgericht bei der Prüfung, ob die fraglichen Bankkundendaten tatsächlich pseudonymisiert worden waren, nur auf die Datenschutzdoktrin und nicht auf das Bankenrecht bezieht.

50 HG150170, E. 5.3.5.1.

51 Dies entspricht auch weitgehend der Praxis: Sowohl die allgemeinen Geschäftsbedingungen der UBS als auch der Credit Suisse halten fest, dass Bankkundendaten an einen im Ausland ansässigen Dienstleister nur übermittelt werden können, wenn sie «keinen Rückschluss auf die Identität des Kunden zulassen» (AGB UBS 2018, Ziff. 12; AGB CS 2017, Ziff. 12).

52 Aus Gründen der Konsistenz innerhalb des Rechtssystems wird die Möglichkeit der Identifizierung unserer Ansicht nach aus der Sicht des Bankgeheimnisses genauso analysiert wie datenschutzrechtlich. Es ist daher angemessen, nicht nur die Mittel zu berücksichtigen, die der Empfänger vernünftigerweise zur Re-Identifizierung der betroffenen Person einsetzen könnte, sondern auch diejenigen, die angemessenerweise von anderen autorisierten Dritten eingesetzt werden könnten (z.B. Behörden, die nach lokalem Recht zum Zugriff auf die Daten berechtigt sind). Reicht die Anonymisierung oder Pseudonymisierung nicht aus, um eine erneute Identifizierung nach diesem Kriterium zu verhindern, unterliegen die Daten weiterhin dem Bankgeheimnis. Dieses hindert als solches nicht daran, die Daten Bankbeauftragten weiterzugeben, die gemäss Art. 47 BankG der Geheimhaltungspflicht unterstehen. Die Übermittlung von Bankkundendaten im Sinne von Art. 47 BankG erfordert jedoch verschiedene Vorsichtsmassnahmen (zu den Vorkehrungen, die im Zusammenhang mit der Übermittlung von geheimhaltungspflichtigen Daten an Anbieter von Cloud-Diensten zu treffen sind, siehe Cloud Guide der SBvG vom März 2019, sowie die dazugehörenden

Fussnoten (Fortsetzung)

Rechtsgutachten (Laux/Hofmann/Schieweck/Hess [Fn. 2]; Isler/Kunz/Müller/Schneider/Vasella [Fn. 2]).

53 In ihrem Rundschreiben 2008/21 über operationelle Risiken schreibt die FINMA vor, dass die Banken einen angemessenen Rahmen schaffen müssen, der die Vertraulichkeit der «Kundenidentifikationsdaten» (CID) gewährleistet. Die FINMA präzisiert, dass Pseudonymisierung und Anonymisierung gerade technische Massnahmen sind, die die Vertraulichkeit gewährleisten (FINMA, Rundschreiben 2008/21, Rn. 12). Diese Daten umfassen direkte Kundenidentifikationsdaten (z.B. Vorname, zweiter Vorname, Nachname), indirekte Kundenidentifikationsdaten (z.B. Passnummer) und potenziell indirekte Kundenidentifikationsdaten (z.B. Kombination von Geburtsdatum, Beruf, Nationalität usw.). Entscheidend ist daher die Identifizierbarkeit des Kunden. Somit stellt a contrario die Offenlegung von Informationen, die keinen Kunden identifizieren, in den Augen der FINMA kein operationelles Risiko dar. Die FINMA hält fest, dass CID, wenn sie ausserhalb der Schweiz gespeichert oder vom Ausland aus abgerufen werden, «angemessen geschützt (z.B. anonymisiert, verschlüsselt oder pseudonymisiert) werden» (FINMA, Rundschreiben 2008/21, Anhang 3, Rn. 20). Darin wird ausdrücklich festgehalten, dass anonymisierte Daten «gemäss Definition keine CID mehr [sind] und nicht unter das DSG» fallen. (FINMA, Rundschreiben 2008/21, Anhang 3, Rn. 65); vgl. auch Fischer Philipp, L'externalisation de services dans le domaine bancaire et financier, SZW 2016, 137 ff.

54 Die FINMA hat sich zur Bedeutung der Kundenidentifikation bei einem Diebstahl von Bankkundendaten im Rahmen eines Enforcementverfahrens geäussert. Sie hob hervor, dass die fehlende Möglichkeit für den Bankkundendatendieb, eine Verknüpfung zwischen bestimmten Kunden zugeordneten Vermögensdaten und den Kundenidentifikationsdaten herzustellen, von entscheidender Bedeutung ist. Vermögensdaten, die an sich keine Identifizierung der betroffenen Person ermöglichen, sind somit nur dann durch das Bankgeheimnis geschützt, wenn sie mit Kundenidentifikationsdaten in Verknüpfung gebracht werden können (FINMA-Bulletin 4/2013, 76).

55 CR CP II-Chappuis Benoît, Art. 321 StGB N 71; Corboz Bernard, Les infractions en droit suisse, Bd. 2, 3. Aufl. 2010, Art. 321 StGB N 69; Trechsel Stefan/Vest Hans, StGB PK, Art. 321 StGB N 23.

56 HG150170, E. 5.3.5.8; BGer 4A_365/2017, E. 521 ff. Ein besser nuancierter Ansatz bei der Verteilung der Beweislast wäre unserer Ansicht nach wünschenswert, Hirsch/Jacot-Guillarmod, 165 ff. (Fn. 1).

57 Zum konkreten Beweisgegenstand ist das Handelsgericht im Wesentlichen der Auffassung, dass die Bank folgende Aspekte hätte nachweisen müssen (HG150170, E. 5.3.5 ff.): (1) die Massnahmen, die ergriffen wurden, um den Zugang zum Konkordanzschlüssel zu beschränken; (2) die Unmöglichkeit für die US-Behörden, die betroffene Person anhand der übermittelten Daten erneut zu identifizieren; und (3) die Unmöglichkeit für die US-Behörden, die betroffene Person durch einen Abgleich der übermittelten Daten mit anderen ihnen zur Verfügung stehenden Informationen zu re-identifizieren. In Bezug auf den ersten Punkt ist das Bundesgericht weniger anspruchsvoll und hält die Verwendung einer pseudonymisierten Kontonummer grundsätzlich für eine geeignete Massnahme, um eine erneute Identifizierung zu verhindern. Nach dieser Massnahme setzt die Re-Identifikation die Verwendung des Konkordanzschlüssels voraus, zu dem das DoJ keinen Zugang hat (BGer 4A_365/2017, E. 5.3.1.). Im Übrigen lässt das Bundesgericht im Hinblick auf den dritten Punkt (Möglichkeit der extrinsischen Gegenprüfung) ausdrücklich offen, wer, die Bank oder der Gesuchsteller, die Beweislast trägt (BGer 4A_365/2017, E. 5.2.2 in fine). Ein kürzlich ergangenes Urteil des Appellationsgerichts des Kantons Basel-Stadt (ZB.2019.3 vom 6. September 2019, E. 4.2.3) besagt, dass die Bank die Beweislast dafür trägt, dass das DoJ nicht in der Lage ist, extrinsische Gegenkontrollen durchzuführen. Nach Ansicht des Appellationsgerichts ist diese Entscheidung notwendig, weil die Wirksamkeit der Pseudonymisierungsmassnahmen von den zusätzlichen Informationen abhängt, die sich im Besitz des DoJ befinden. Das Appellationsgericht weist jedoch darauf hin, dass einer Partei nach den Regeln von Treu und Glauben eine Mitwirkungspflicht auferlegt werden kann, um eine positive Tatsache nachzuweisen, die die Verwirklichung der betreffenden negativen Tatsache verhindert (ZB.2019.3 vom 6. September 2019, E. 4.3.4). Im vorliegenden Fall hat die Bank vor Einreichung ihrer Replik nicht behauptet, dass die strittigen Daten pseudonymisiert seien; von der Gegenpartei konnte daher nach den Regeln von Treu und Glauben nicht verlangt werden, dass sie die erforderlichen Beweise für die gegenteilige Behauptung, nämlich die Möglichkeit für das DoJ, extrinsische Gegenkontrollen durchzuführen, vorlegt (ZB.2019.3 vom 6. September 2019, E. 4.3.4).